Netfilter: utilizzo di *iptables* per intercettare e manipolare i pacchetti di rete

Giacomo Strangolino

Sincrotrone Trieste

http://www.giacomos.it

delleceste@gmail.com

Sicurezza delle reti informatiche

- **<u>Primi decenni di esistenza</u>**:

•ricercatori universitari per scambio di messaggi elettronici;

•dipendenti di industrie per la condivisione delle stampanti.

.

Sicurezza delle reti informatiche (II)

- **Oggi**:
- segretezza
- autenticazione
- non disconoscimento (*firma*)
- controllo di integrità

.

Sicurezza delle reti informatiche (III)

- **Oggi**:

•virus informatici

spyware/malware

•keylogger

esegue determinate operazioni: visualizzazione di pubblicità, raccolta di informazioni personali, modifica della configurazione del computer, in genere senza prima richiedere l' autorizzazione.

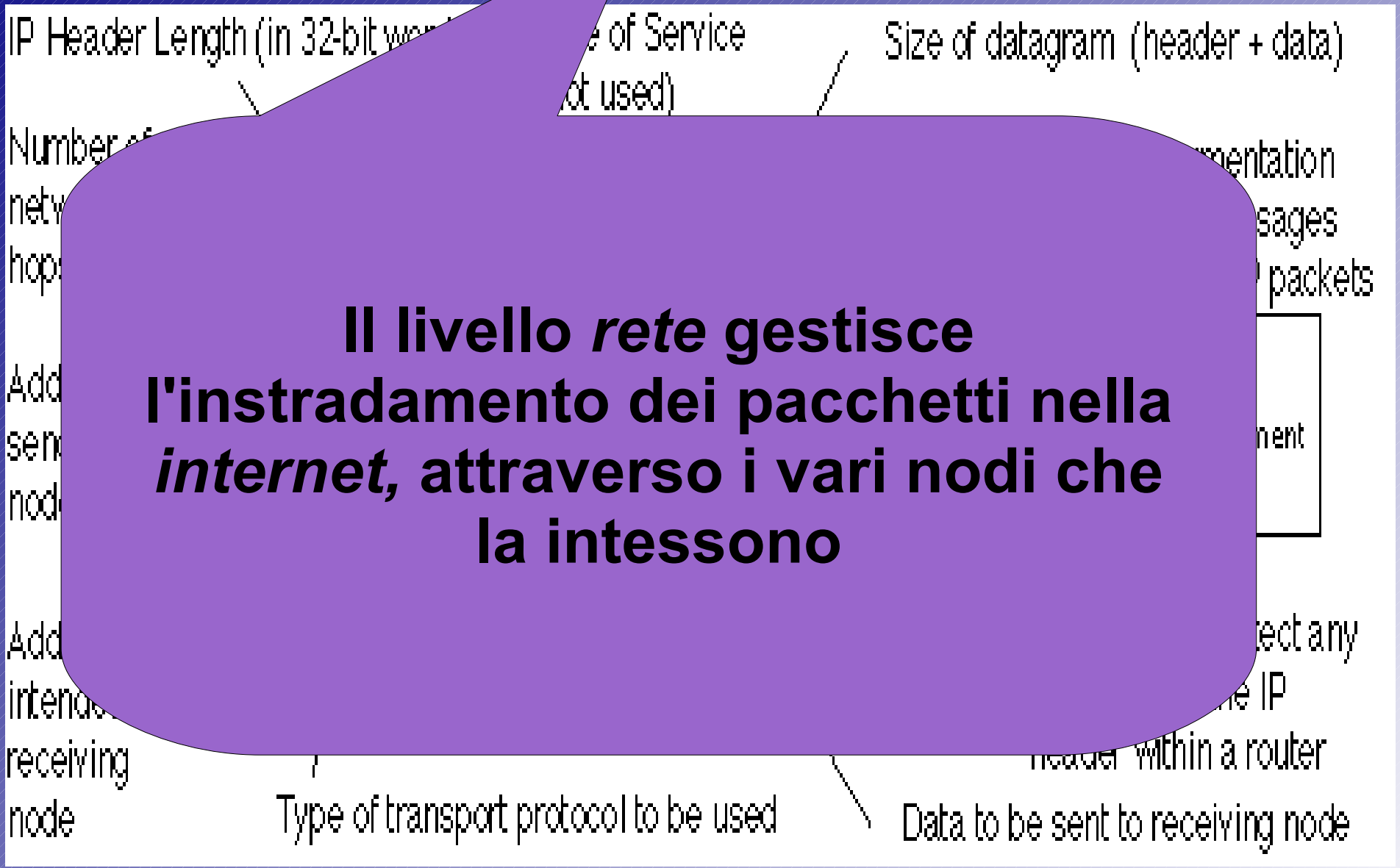
registra la pressione dei tasti sulla tastiera.

L'architettura stratificata delle reti informatiche e la sicurezza

L'architettura stratificata delle reti informatiche e la sicurezza

L'architettura stratificata delle reti informatiche e la sicurezza

Architettura: livello *rete*



Il livello *rete* gestisce l'instradamento dei pacchetti nella *internet,* attraverso i vari nodi che la intessono

Firewall: la sicurezza al livello rete

- In azienda **le informazioni private** (segreti commerciali, piani di sviluppo, strategie di marketing, analisi finanziarie) **non devono essere divulgate;**
- pericolo che informazioni entrino (virus e altri agenti nocivi digitali)

.

Firewall: la sicurezza al livello rete (II)

- Implementa un filtro di pacchetti: tabelle con regole che elencano sorgenti e destinazioni accettabili e vietate

Firewall: la sicurezza al livello rete (III)

•**Problemi**:

• **bloccare i pacchetti in uscita non è facile:**

• i servizi non sono obbligatori, ascolto su

•in alcuni servizi in ... sono as...

• **per quanto rig... si sa circa ciò che vog... no tutto il t...**

Inconveniente: se si desiderano certi servizi, è necessario aprire delle porte

L'architettura stratificata delle reti informatiche e la sicurezza

Architettura: il trasporto

- **TCP (Transmission Control Proto controllo della trasmissione):**

Gestisce la ritrasmissione e il controllo del flusso

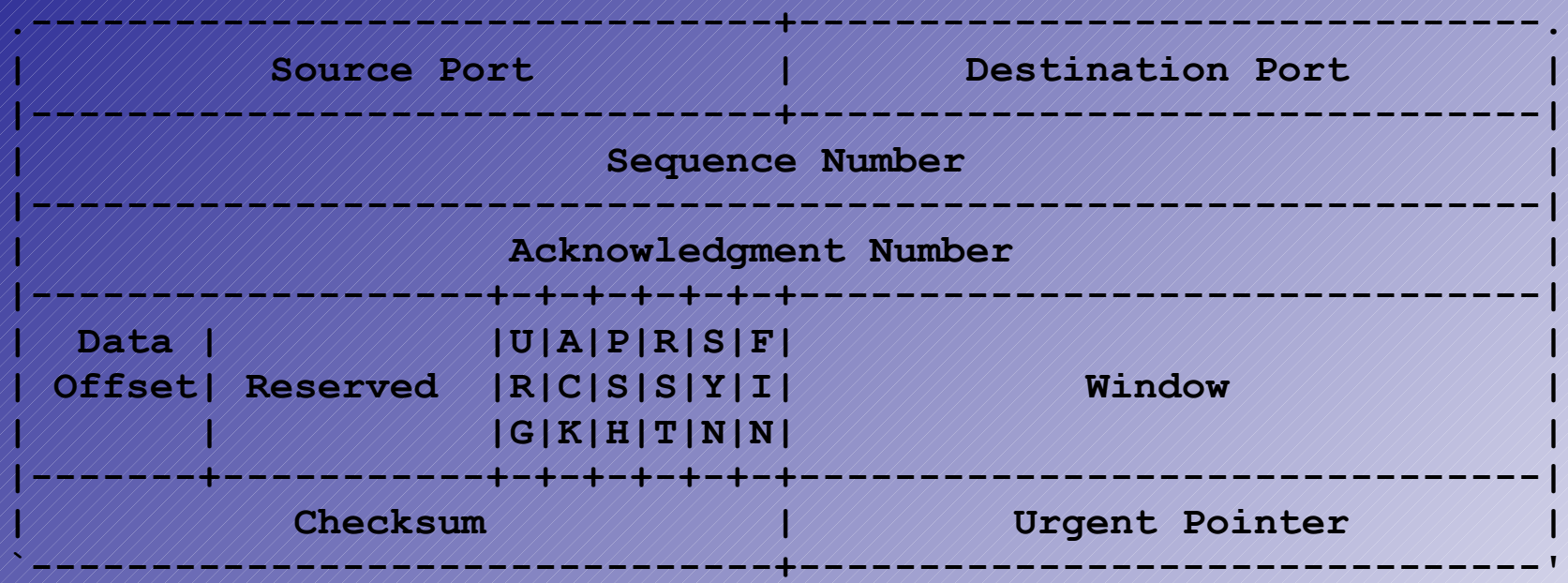
  - **È affidabile e orientato alla connessione.**

- **UDP (User Datagram Protocol):**

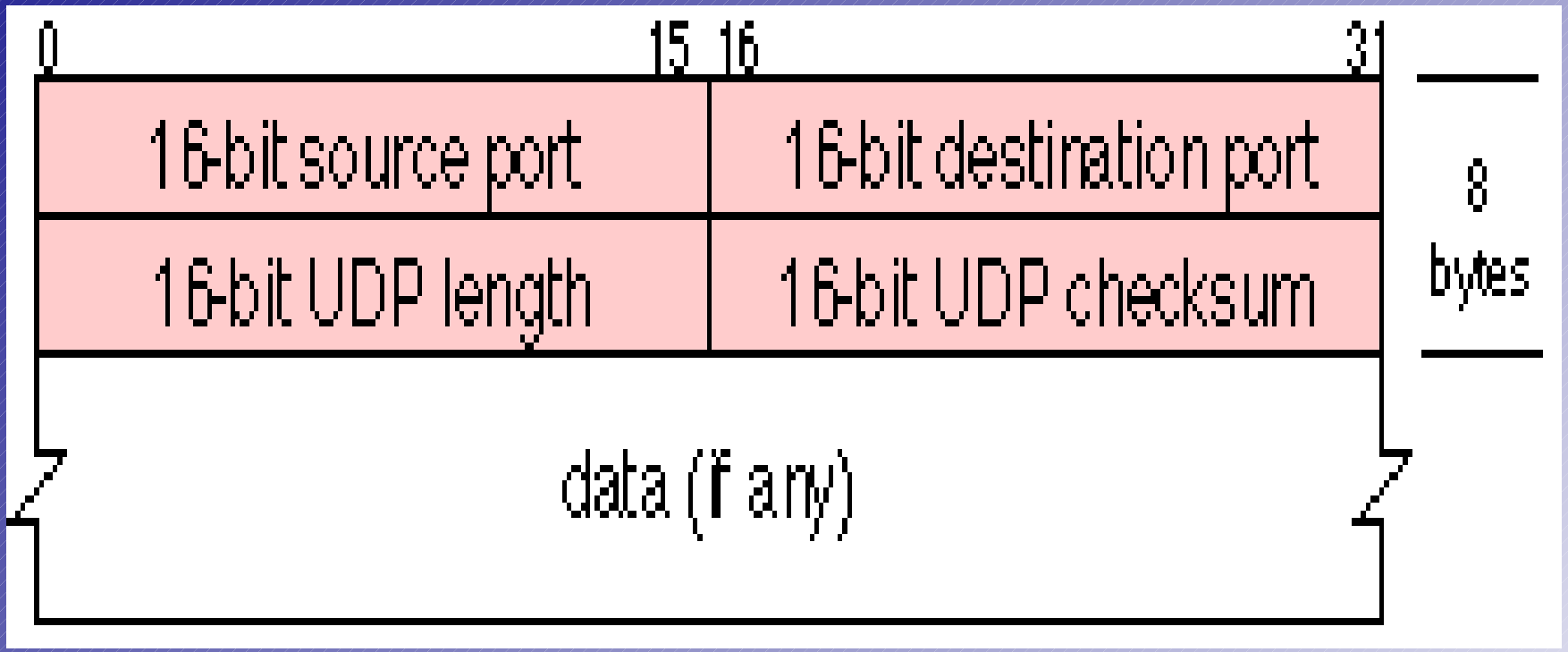
È veloce!

  - **Non è affidabile, non è orientato alla connessione ed è senza riscontro .**

Intestazione TCP



Intestazione UDP



L'architettura stratificata delle reti informatiche e la sicurezza

***Netfilter/iptables*: l'infrastruttura per il *firewalling* in linux**

- *netfilter*: il motore in spazio *kernel* (packet filtering, address translation, packet mangling, estensioni)
- *iptables*: utilità in spazio utente per la configurazione di netfilter

Funzionalità

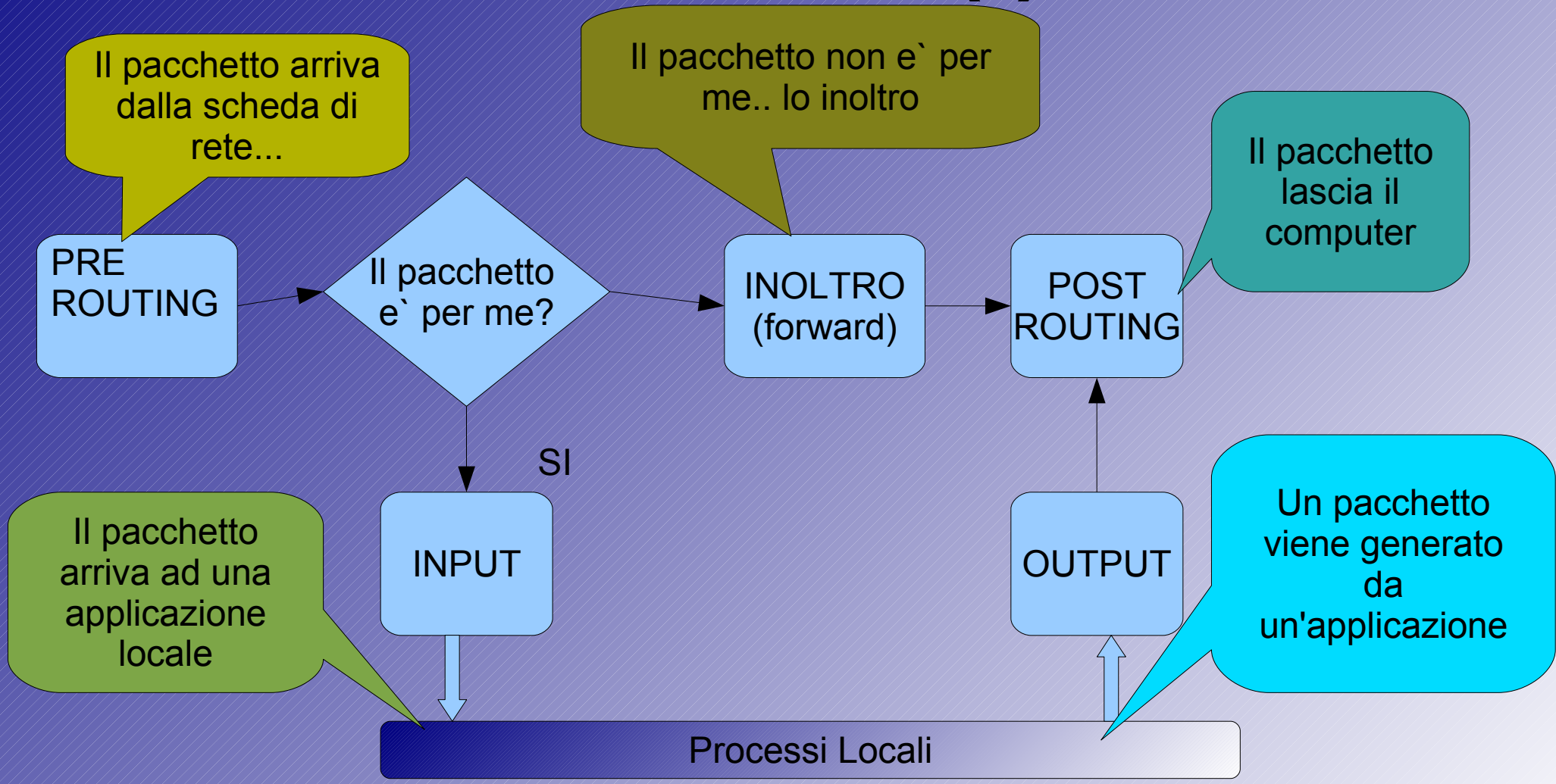
- Stateless packet filtering (IPv4 e IPv6);
- stateful packet filtering (IPv4 e IPv6);
- tutti i tipi di traduzione degli indirizzi e delle porte, e.g. NAT/NAPT (solo IPv4);
- infrastruttura flessibile e estensibile;
- API multilivello disponibile per estensioni di terze parti

.

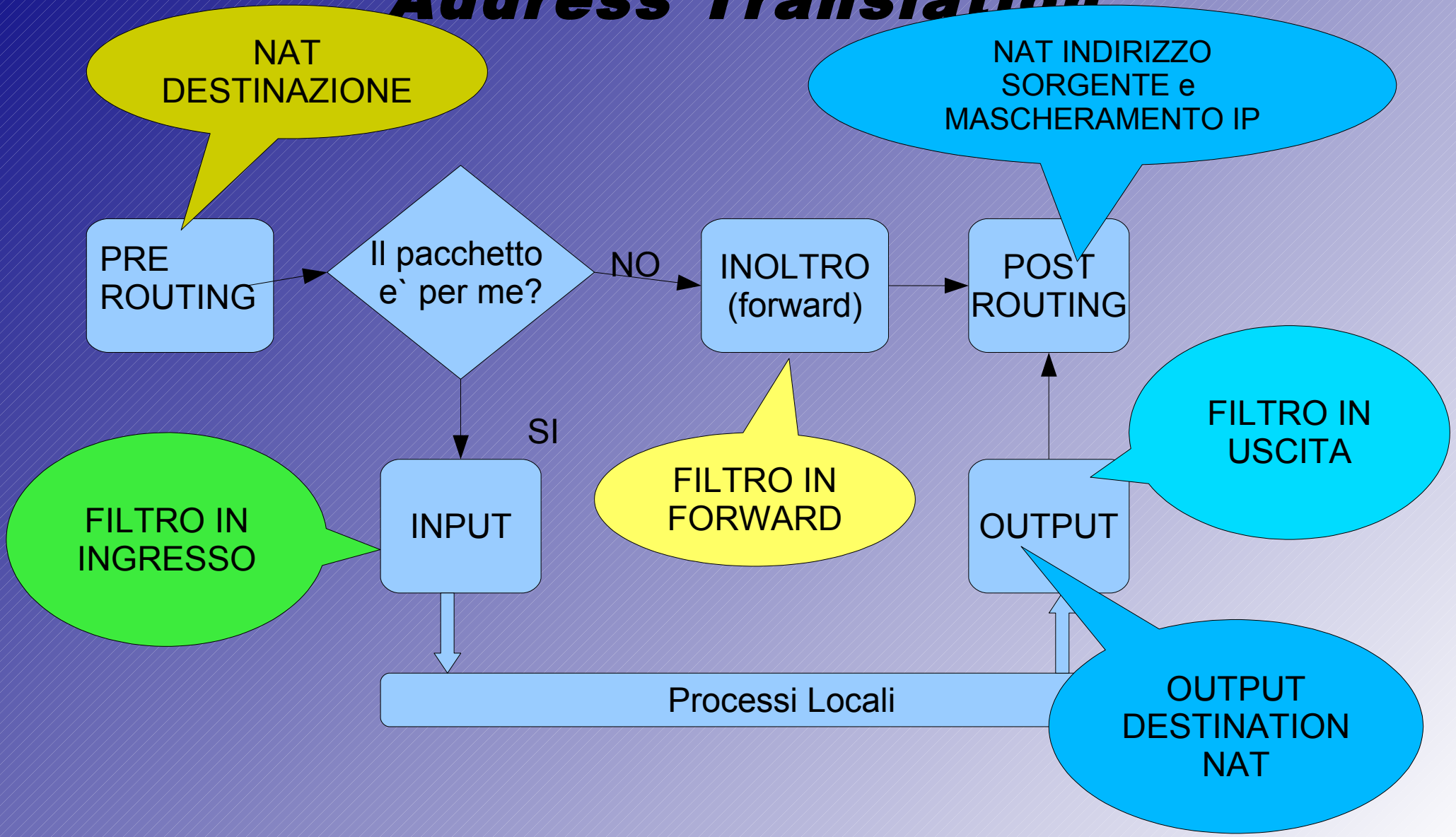
Utilizzazione

- implementazione di un **filtro di pacchetti** basato su regole *stateless* e *stateful*;
- utilizzazione del **NAT** e del *mascheramento* degli indirizzi per condividere l'accesso *Internet* di una connessione via modem;
- implementarzione *transparent proxies*;
- manipolazione dei pacchetti di rete (*packet mangling*) alterando ad esempio i bit TOS/DSCP/ECN dell'intestazione IP

L'architettura di rete e l'instradamento dei pacchetti nel *kernel* linux (I)



L'architettura di rete e l'instradamento dei pacchetti nel *kernel* linux (II): *filtering* e *Network Address Translation*



IPTABLES: concetti fondamentali

- 2 *target* (obiettivi) principali: ***ACCEPT*** e ***DROP***;
- 3 “catene” (percorsi) predefinite: ***INPUT***, ***OUTPUT*** e ***FORWARD*** e altre definibili dall'utente;
- 3 “tabelle”: ***FILTER***, ***NAT***, ***MANGLE***;

.

IPTABLES: concetti fondamentali (II)

- quando si verifica una **corrispondenza** tra il **pacchetto** di rete e la **regola**, la sorte del pacchetto è definita;
- per le regole definite dall'utente, quando si verifica una corrispondenza, il pacchetto salta alla nuova catena definita dall'utente e la percorre *in toto*;
- se non si verifica una corrispondenza, la ricerca continua da dove si era eseguito il salto iniziale.

IPTABLES: inizializzazione del firewall

- **Inizializzazione delle tabelle di *iptables:***

- *iptables -t filter -F*
- *iptables -t nat -F*
  - **Impostazione della politica predefinita**:
- *iptables -P INPUT DROP*
- *iptables -P OUTPUT DROP*
- *iptables -P FORWARD DROP*
  - **Lista delle regole del firewall:**
- *iptables [-t filter] -L*
- *iptables -t nat -L*

IPTABLES: indirizzi di rete

- **specificare un indirizzo sorgente:**

--source/--src

- *iptables -A INPUT -s 192.168.0.2 -j ACCEPT*
- *iptables -A INPUT -s 192.168.0.0/255.255.255.0 -j ACCEPT*

- ***specificare un indirizzo dest***

inversione (“*not*”)

- *iptables -A OUTPUT -d ! 192.168.0.2 -j ACCEPT*
- *iptables -A OUTPUT -d 192.168.0.0/255.255.255.0 -j ACCEPT*

--destination/--dst

IPTABLES: interfacce di rete

--in-interface

- **specificare un'interfaccia di rete:**
  - *iptables -A INPUT -s 192.168.0.2* ***-i eth0*** *-j ACCEPT*
  - *iptables -A INPUT -s 192.168.0.0/255.255.255.0 -j ACCEPT*
- ***specificare un indirizzo des***

--out-interface

  - *iptables -A OUTPUT -d* ***!*** *192.168.0.2* ***-o eth1*** *-j ACCEPT*
  - *iptables -A* ***FORWARD*** *-d 192.168.0.0/255.255.255.0* ***-i eth0 -o eth1*** *-j ACCEPT*

IPTABLES: protocollo di trasporto

- **specificare un protocollo:**

- *iptables -A INPUT **-p tcp** -s 192.168.0.2 -i eth0 -j ACCEPT*

- *iptables -A INPUT **-p udp** -s 192.168.0.0/255.255.255.0 -j ACCEPT*

- *iptables -A OUTPUT **-p icmp -o eth1** -j ACCEPT*

IPTABLES: protocollo di trasporto

· **specificare una porta:**

- *iptables -A INPUT -p tcp -s 192.168.0.2 --**source-port 22** -i eth0 -j ACCEPT*

·*iptables -A OUTPUT **-p udp** --**destination-port 22** -o eth1 -j ACCEPT*

· ***opzioni TCP:***

· *iptables -A INPUT -p tcp --**tcp-flags ALL SYN,ACK** -j DROP*

da esaminare

devono essere attivi

IPTABLES: *stateful connection*

- *Iptables* nei moduli della "*connection tracking*" implementa una macchina a stati che traccia lo stato di ciascuna connessione;
- Per attivare le opzioni di *ip_conntrack*, è sufficiente attivare il modulo con l'opzione ***-m state***;

.

IPTABLES: *stateful connection (II)*

- Gli stati rintracciabili in una connessione sono:
  - ***NEW***: un pacchetto crea una connessione;
  - ***ESTABLISHED***: un pacchetto appartiene a una connessione esistente;
  - ***RELATED***: un pacchetto in relazione a una connessione esistente, ma di cui non fa parte (es. *ftp "data"* o errore *ICMP*);
  - ***INVALID***: un pacchetto il cui stato non può essere identificato (solitamente sono scartati)

.

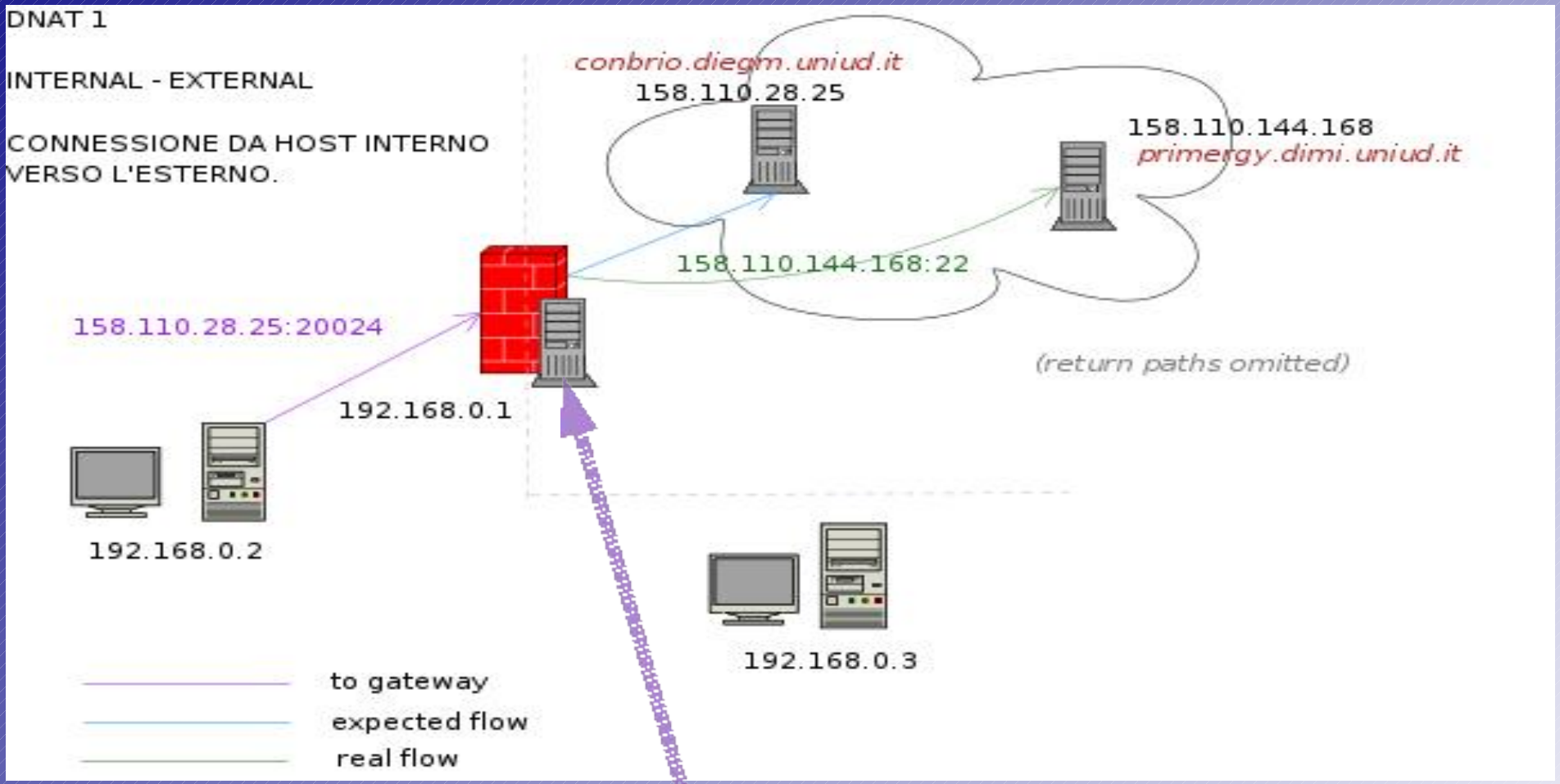
IPTABLES: *stateful connection (III): esempi*

- **Blocco delle connessioni nuove o invalide in ingresso**:
- *iptables -A INPUT -i ppp0* ***-m state --state NEW, INVALID*** *-j DROP*
- *iptables -A FORWARD -i ppp0 -o eth0* ***-m state --state NEW, INVALID*** *-j DROP*
- ***Permesso alle connessioni nuove in uscita o già stabilite:***
- *iptables -A OUTPUT -o ppp0* ***-m state --state NEW*** *-j ACCEPT*
- *iptables -A INPUT -i ppp0* ***-m state --state RELATED,ESTABLISHED*** *-j ACCEPT*

IPTABLES: *NETWORK ADDRESS TRANSLATION (NAT)*

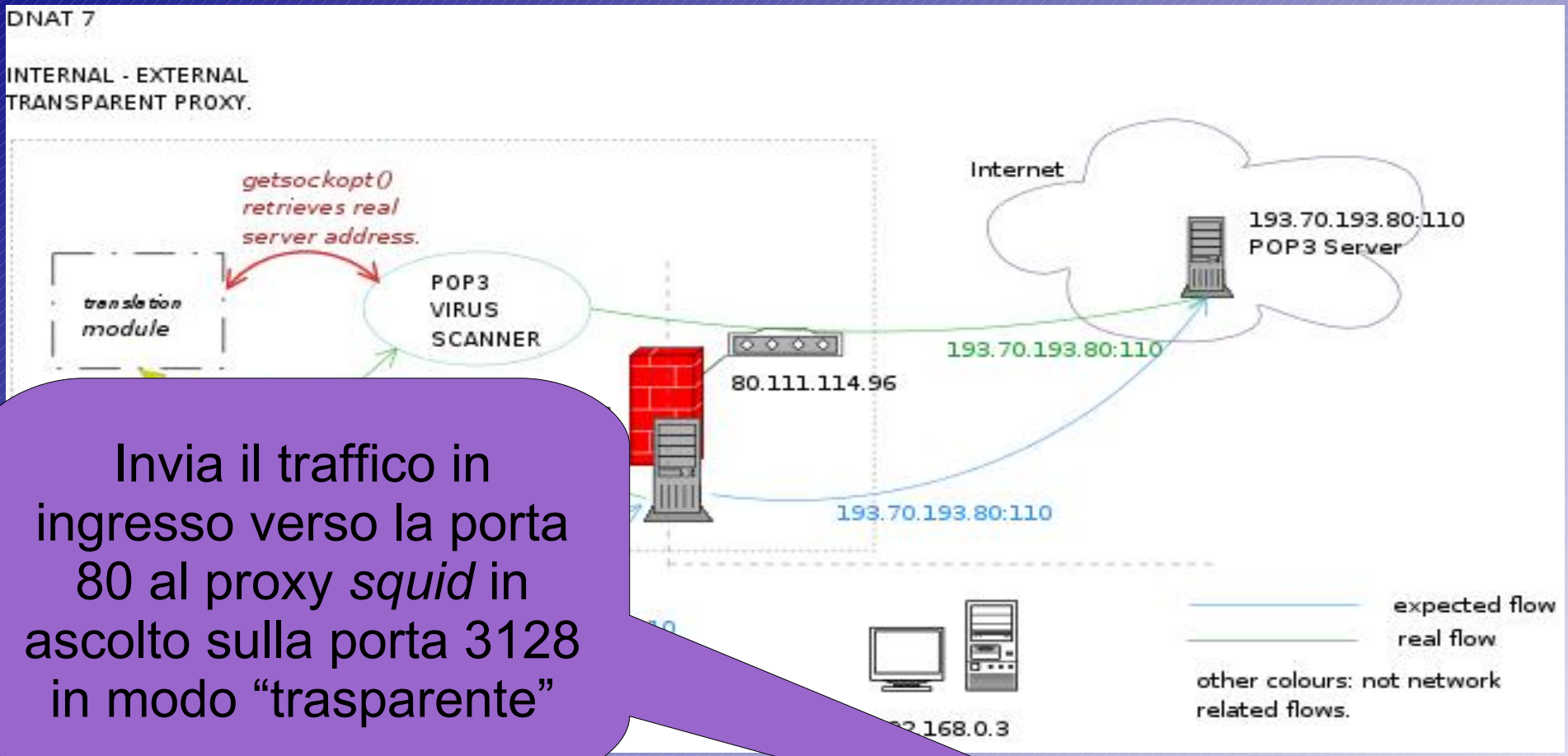
- Il **NAT** consente la modifica degli indirizzi IP sorgente o destinazione o delle porte sorgente o destinazione, cosicché diviene possibile indirizzare un pacchetto a una destinazione diversa da quella per cui era stato creato oppure a un servizio diverso, rispettivamente.

IPTABLES: *NETWORK ADDRESS TRANSLATION (NAT)* (II)



iptables -A PREROUTING -t nat -p tcp -d 158.110.28.25 --dport 20024 -j DNAT --to 158.110.144.168:22

IPTABLES: *TRANSPARENT PROXY* (caso particolare di *DNAT*)



Invia il traffico in ingresso verso la porta 80 al proxy *squid* in ascolto sulla porta 3128 in modo "trasparente"

- *iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 110 -j **REDIRECT** --to-port 8110*
- *iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j **REDIRECT** --to-port 3128*

IPTABLES: CONDIVISIONE DELLA CONNESSIONE INTERNET VIA MODEM

- Accade spesso di avere più computer connessi alla rete *Internet* attraverso un modem:
- con *iptables* è semplice permettere a tutti i PC di accedere alla rete usando il cosiddetto *mascheramento degli indirizzi* (*ip masquerading*):
- ***iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE***

Tutto il traffico in uscita attraverso l'interfaccia *ppp0* viene mascherato

IPTABLES: RIMOZIONE DI UNA REGOLA

- Si può cancellare una regola ripetendo la sintassi specificata al momento del suo inserimento, cambiando ***-A*** con ***-D***:
  - ***iptables -D INPUT -s 192.168.0.2 -j ACCEPT***
- Se ci sono più regole con le stesse opzioni nella stessa catena, verrà cancellata solo la prima.

IPTABLES: ALTRI ESEMPI

Modulo multiport

- Opzione *multiport: posso indicare più porte nella stessa regola:*

•***iptables -A INPUT -p tcp -m multiport --dports telnet,www,dns -j ACCEPT***

•Opzione ***LOG*****:** registrare le operazioni di *iptables* sul file di log

- *iptables -A INPUT -i ppp0* ***-m state --state NEW, INVALID*** *-j LOG –log-prefix “conn. new/inval. da ppp0”*

- *iptables -A INPUT -i ppp0* ***-m state --state NEW, INVALID*** *-j DROP*

Limite di 29 caratteri nella stringa!

IPTABLES: ESTENSIONI

- Modulo **time**: consente di attivare delle regole in base all'orario ed ai giorni della settimana:

- ***iptables -A INPUT -p tcp --dport www -m time –timestart 09:00 –timestop 18:00 –days Mon,Tue,Wed,Thu,Fri -j ACCEPT***

- Modulo **ipp2p**: co… in merito al traffico *peer to pe*… può rilevare il traffico generato dai …cipali sistemi di file sharing:

- ***iptables -A PREROUTING -t nat -s 192.168.1.0/24 -m ipp2p –edk -j ACCEPT***

- ***iptables -A PREROUTING -t nat -s 192.168.1.0/24 -m ipp2p –kazaa –bit –winmx --gnu -j DROP***

Consente di usare programmi di file sharing come eDonkey o eMule

Nega il traffico legato a programmi come *kazaa*, *Bit-Torrent*, *WinMX*, *Gnutella*

IPTABLES: AIUTOOO!!!

- ***iptables -p tcp –help***

• Le regole che contengono ***-A FORWARD*** richiedono che nel kernel sia abilitato l'inotro dei pacchetti di rete attraverso le interfacce:

- ***echo 1 > /proc/sys/net/ipv4/ip_forward***

- ***http://www.netfilter.org/***

IPTABLES AVANZATO: IP QUEUE

- Il modulo di *netfilter* denominato ***QUEUE*** consente di mandare i pacchetti in una coda in spazio utente e di scrivere applicativi che, ponendosi in ascolto su quella coda, possono ricevere e analizzare i pacchetti, nonché finalmente esprimere un verdetto per ciascuno di essi.

- Questo estende le funzionalità del *firewall* consentendo all'utente di personalizzare totalmente il funzionamento del filtro di pacchetti

IPTABLES AVANZATO: IP QUEUE (II)

- Ad esempio, le regole:

- i***ptables -A INPUT -i ppp0 -j QUEUE***

- ***iptables -A OUTPUT -o ppp0 -j QUEUE***

consentono di inviare ad un'applicazione in ascolto in spazio utente tutti i pacchetti che attraversano l'interfaccia di rete *ppp0*, e di affidare ad essa la sorte di ciascuno di essi.

- **Vedere esempio** di applicazione

Netfilter: utilizzo di *iptables* per intercettare e manipolare i pacchetti di rete

Giacomo Strangolino

Sincrotrone Trieste

http://www.giacomos.it

delleceste@gmail.com